UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

NEVILLE MCFARLANE, EDWARD HELLYER, DEANNA COTTRELL, CARRIE MASON-DRAFFEN, HASEEB RAJA, RONNIE GILL, JOHN FRONTERA, SHARIQ MEHFOOZ, and STEVEN PANICCIA, individually and on behalf of all others similarly situated, Plaintiffs, v. ALTICE USA, INC., a New York Corporation, Defendant.	Lead Case No. 20-CV-1297 (consolidated with 20-CV-1410)

PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS AND MOTION TO COMPEL ARBITRATION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Regulations

Plaintiffs Neville McFarlane ("McFarlane"), Deanna Cottrell ("Cottrell"), Edward Hellyer ("Hellyer"), Carrie Mason-Draffen ("Mason-Draffen"), Haseeb Raja ("Raja"), Ronnie Gill ("Gill"), John Frontera ("Frontera"), Shariq Mehfooz ("Mehfooz"), and Steven Paniccia ("Paniccia"), individually and on behalf of the putative class, (collectively, "Plaintiffs"), submit this Opposition to Defendant's Motion to Dismiss Plaintiffs' Amended Consolidated Complaint and Memorandum in Support (Dkt. No. 46) ("MTD") and Motion to Compel Arbitration and Memorandum in Support (Dkt. No. 48) ("MTCA").

I. SUMMARY OF FACTUAL ALLEGATIONS

Altice USA, Inc. ("Altice" or "Defendant") is one of the largest cable TV and communications providers in the United States. ¶ 1.[1] Plaintiffs are current and former employees of Altice, some of whom were also cable subscribers, who entrusted Altice with their sensitive personally identifiable information ("PII"). In February 2020, Altice notified current and former employees (as well as the attorneys general of several states) that in November 2019, a successful phishing campaign compromised Altice's corporate email accounts. According to Altice, once these hackers were inside Altice's corporate email accounts, they were able to "access" and "download" a report containing the unencrypted PII of 52,846 current and former Altice employees (some of whom were also Altice cable subscribers), including their employment information, dates of birth, Social Security numbers, and some drivers' license numbers (the "Data Breach" or the "Breach"). ¶¶ 6-7. Thus, as a result of Defendant's failure to implement adequate IT security measures that reasonably conformed with industry standards, hackers have now accessed, downloaded, and used the unencrypted private and confidential information, including Social Security numbers, of Plaintiffs and the Class. ¶¶ 93-102, 147-60; *see* ¶¶ 17, 73, 84.

[1] All "¶" and "¶¶" references are to the Amended Consolidated Class Action Complaint ("Complaint") unless otherwise specified.

II. PLAINTIFFS SUFFERED INJURY-IN-FACT AND THUS HAVE ARTICLE III STANDING

To establish standing at the pleading stage, the complaint must allege facts demonstrating that the plaintiffs "have (1) suffered an injury in fact; (2) that is fairly traceable to the challenged conduct of a defendant; and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). Defendant argues that Plaintiffs fails to establish the first element: injury-in-fact. Contrary to Defendant's contention, Plaintiffs have pled sufficient allegations to establish injury-in-fact.

An injury-in-fact is "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id.* at 1548.

All Plaintiffs adequately allege that their highly sensitive PII, including names, dates of birth, and Social Security numbers, was exposed to cyber criminals at the hands of Altice. ¶¶ 13-88; *see also* Exhibits 1-3 to Complaint. As a result, Plaintiffs have suffered several separate injuries that each independently confers Article III standing.

A. The Alleged Identity Theft Constitutes Injury-In-Fact

Plaintiffs McFarlane, Mehfooz, and Paniccia sufficiently allege injury-in-fact based on the theft and misuse of their identities immediately following the Altice Data Breach.

McFarlane, Mehfooz, and Paniccia allege that their PII, including names, dates of birth, and Social Security numbers, were disclosed to cyberhackers during the Data Breach at Altice. ¶¶ 13-20, 69-88. Plaintiffs McFarlane, Mehfooz, and Paniccia further allege that their PII was misused directly following the Data Breach. Specifically, on January 12, 2020—two months after the Data Breach—Plaintiff McFarlane discovered that a credit card was fraudulently opened in his name, and he then discovered in March 2020 that an identity thief had attempted to change his home address. ¶ 17. In mid-December 2019—one month after the Data Breach—Plaintiff

Paniccia discovered that someone was using his PII to fraudulently open a credit card in his name. ¶¶ 84-85. On March 23, 2020, while applying to refinance his home, Plaintiff Mehfooz discovered that someone had opened an unauthorized credit card in his name through Merrick Bank, which harmed his credit score and interrupted his home refinancing process. ¶¶ 73-75. Plaintiffs have not been victims of other data breaches that compromised this PII. ¶¶ 20, 79, 88. Accordingly, Plaintiffs McFarlane, Mehfooz, and Paniccia have adequately alleged that they suffered identity theft and misuse of their PII as a result of the Data Breach.

The misuse of sensitive identifying data *alone* is sufficient to confer standing. *See Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012) (holding that the misuse of plaintiff's sensitive information to open a bank account was sufficient to confer standing even though she did not allege any "unreimbursed losses"); *cf. Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) (finding injury-in-fact for data breach case and defining "actual misuse" as a "fraudulent charge"). Indeed, as the Fourth Circuit recently held:

> [Plaintiffs here] allege that they have already suffered actual harm in the form of identity theft and credit card fraud. The Plaintiffs have been concretely injured by the data breach because the fraudsters used—and attempted to use—the Plaintiffs' personal information to open Chase Amazon Visa credit card accounts without their knowledge or approval. Accordingly, *there is no need to speculate on whether substantial harm will befall the Plaintiffs*.

Hutton v. Nat'l Bd. of Examiners in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018) (emphasis added).

While Defendant cites *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017) to argue that Plaintiffs McFarlane and Paniccia lack standing because they do not allege that they were required "to make any payments" as a result of the identify theft (MTD at 7 n.1), Defendant's argument is unconvincing. In *Whalen*, the Court emphasized that the data breach only exposed plaintiff's credit card number, which "was promptly canceled after the breach and no other

personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen." *Id.* at 90. It was in that limited scenario, where the only alleged misuse was of plaintiff's credit card information (which plaintiff quickly rendered *unusable*), that the court in *Whalen* deemed the misuse alone to be insufficient. But where, as here, Plaintiffs allege that their *permanent identifying information* (such as date of birth and Social Security number) was misused to open unauthorized credit cards, it is not necessary for Plaintiffs to allege that they suffered unreimbursed economic harm. *See, e.g.*, *Hutton,* 892 F.3d at 622 (standing conferred based on alleged fraudulent use of identifying information, without alleged unreimbursed charges, because "the Supreme Court long ago made clear that 'in interpreting injury in fact ... standing [is] not confined to those who [can] show economic harm.'") (quoting *United States v. Students Challenging Regulatory Agency Procedures*, 412 U.S. 669, 686 (1973)); *Resnick*, 693 F.3d at 1324 (similar); *see also Stollenwerk v. Tri-West Health Care All.*, 254 F. App'x 664, 667 (9th Cir. 2007) (plaintiff established that breach proximately caused identity theft where credit accounts were fraudulently opened six weeks after defendant's systems were compromised). Indeed, the Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted *using the identifying information of another person without authority*." 17 C.F.R. § 248.201 (2013). Thus, the unauthorized use of someone's confidential *identifying* information, like the fraudulent credit cards opened in the names of Plaintiffs McFarlane, Mehfooz, and Paniccia, *is identity theft*.

Plaintiffs McFarlane, Mehfooz, and Paniccia have alleged injury-in-fact based on the theft of their identities to open unauthorized financial accounts.

B. Plaintiffs Allege Injury-in-Fact Based on the Substantial Risk of Future Harm

"A party facing prospective injury has standing to sue where the threatened injury is real, immediate, and direct." *Davis v. Fed. Election Comm'n*, 554 U.S. 724, 734 (2008). An allegation

of threatened injury in the future is sufficient to establish standing "if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014). Supreme Court precedent does not "uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about"—hence, the "substantial risk" standard. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013). Ultimately, the purpose of the imminence requirement is "to ensure that the court avoids deciding a purely hypothetical case[.]" *Baur v. Veneman*, 352 F.3d 625, 632 (2d Cir. 2003).

Applying these principles in the context of a data breach case, this Court in *Sackin v. TransPerfect Global, Inc.*, 278 F. Supp. 3d 739 (S.D.N.Y. 2017) held that "allegations that Defendant has provided Plaintiffs' names, addresses, dates of birth, Social Security numbers and bank account information *directly to cyber-criminals* creates a risk of identity theft sufficiently acute so as to fall comfortably into the category of 'certainly impending.'" *Id.* at 746 (emphasis added). The Court reasoned:

> The most likely and obvious motivation for the hacking is to use Plaintiffs' PII nefariously or sell it to someone who would. *See Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."). Circuit courts addressing this issue consistently have held that Article III does not require Plaintiffs to wait for their identities to be stolen before seeking legal recourse. *See Attias v. Carefirst, Inc.*, 865 F.3d 620, at 629-30 (D.C. Cir. 2017) (holding that alleged increased risk of identity theft was sufficiently imminent to establish standing after a retailer's data breach); *Remijas*, 794 F.3d at 695 (same); *Galaria v. Nationwide Mut. Ins.*, 663 Fed. Appx. 384, 388 (6th Cir. 2016) (same); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164 (1st Cir. 2011) (same).

Id. Thus, the Court concluded that "[w]hile the Second Circuit has yet to address the question, two recent unreported decisions suggest that it will follow the lead of its sister circuits." *Id.* (citing *Katz v. Donna Karan Co.*, 872 F.3d 114, 120-21 (2d Cir. 2017); *Whalen*, 689 Fed. Appx. at 90. In distinguishing *Whalen* and *Katz*, the Court in *Sackin* emphasized that the allegations before it were

that the defendant "divulged information—including *birth dates and social security numbers*—far more sensitive than all or a portion of a credit card number, and that the PII here was *provided directly to cybercriminals*, and not merely printed on a store receipt." *Id.* at 746 (emphasis added); *See also Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 340 (W.D.N.Y. 2018) ("*Whalen* strongly implies that the Second Circuit would follow those circuits that have held that a risk of future identity theft is sufficient to plead an injury in fact.").

Here, similar to the allegations in *Sackin*, cybercriminals specifically targeted Altice, intentionally devoted considerable time and effort to conducting a successful phishing campaign on numerous Altice employees, used stolen credentials to hack into Altice's corporate accounts, and then accessed and even *downloaded* a report containing the unencrypted PII of more than 52,000 former and current Altice employees. ¶¶ 93-102. Thus, as in *Sackin*, Altice allowed Plaintiffs' PII to be disclosed *directly to* hackers where "the most likely and obvious motivation for the hacking [wa]s to use Plaintiffs' PII nefariously or sell it to someone who would." *Sackin*, 278 F. Supp. 3d at 746. In fact, Plaintiffs' allegations are in many ways stronger than those in *Sackin* because here, three Plaintiffs have already had their PII misused within weeks or months of that same PII being accessed and downloaded by cyberhackers in the Data Breach. ¶¶ 17, 73, 84. *See Steven v. Carlos Lopez & Assoc., LLC*, 18-cv-6500, 2019 WL 6252347, at *3 (S.D.N.Y. 2019) (finding that an alleged risk of future identity theft is bolstered where "at least one named plaintiff alleged actual misuse of his or her personal information by the suspected data thief") (citing cases); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 459 (D. Md. 2020) (finding that *some* plaintiffs' allegations of unauthorized financial cards "bring the actual and threatened harm out the realm of speculation and into the realm of sufficiently imminent and particularized harm to satisfy the injury-in-fact…for *all* Bellwether Plaintiffs").

While Defendant cites *Beck v. McDonald*, 848 F.2d 262 (4th Cir. 2017) to argue that the Court here would be required to engage in an "'attenuated chain of possibilities'" to arrive at a substantial risk of harm, Defendant's argument is unpersuasive. In *Beck,* the facts were merely that a laptop containing "names, birth dates, [and] the last four digits of social security numbers" had been "misplaced or stolen." *Id.* at 267. The court found that because "even after extensive discovery" the plaintiffs had "uncovered *no* evidence that the information contained on the stolen laptop has been accessed or misused *or* that they have *suffered identity theft*, nor, for that matter, that the thief stole the laptop with the intent to steal their private information," their allegations were "too speculative." *Id.* at 274. But this is *not* the situation Plaintiffs allege. Instead, Plaintiffs allege that hackers intentionally conducted a phishing campaign against Altice, that these hackers then actively accessed and *downloaded* the contents of an Altice account containing Plaintiffs' unencrypted PII, and that three named Plaintiffs experienced actual identity theft following this Data Breach. ¶¶ 17, 73, 84. Thus, Plaintiffs' allegations are substantially similar to allegations that the court in *Beck* found *did* "suffice[] to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Id.* at 274 (discussing other data breach cases).

In *Steven v. Carlos Lopez & Assoc., LLC*, 18-cv-6500, 2019 WL 6252347 (S.D.N.Y. 2019), another case cited by Defendant, this Court recognized that "where data is intentionally stolen by a hacker 'it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the … data breach.'" *Id.* at *3 (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692, 693 (7th Cir. 2015)). The Court further explained that:

> *[W]here an "unauthorized party" has accessed personally identifying data "it is plausible … to infer that this party has both the intent and the ability to use that data for ill…..* No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; *a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken*."

Id. (quoting *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017)) (emphasis added). In finding that the facts before it did not suffice to allege injury-in-fact, the Court in *Carlos Lopez* reasoned that plaintiffs "allege only that their data was compromised by an errant email sent within [the company]." *Id.* The Court emphasized that the plaintiffs "do not allege that their data was compromised as a result of a hack or some other criminal act," do not allege "that their data was actually viewed, downloaded, copied, or shared," and do not allege that "'any class members' identity' was 'stolen as a result of the breach." *Id.* (citation omitted). In so holding, the Court suggested that allegations of an intentional hack, that personally identifiable data was downloaded, and that certain class members had their data misused subsequent to the hack *would* suffice to allege a substantial risk of harm. Because Plaintiffs here allege *precisely* these facts in the Complaint, Plaintiffs have sufficiently pled a substantial risk of harm. *See* ¶¶ 17, 73, 84, 93-102. The other, mostly out of circuit, cases relied upon by Altice (MTD at 9-10) involved significantly different facts and simply do not suggest that the Court should find a lack of injury in *this* case.[2]

[2] *See, e.g., Hammond v. The Bank of New York Mellon Corp.*, No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *2, *6 (S.D.N.Y. June 25, 2010) (finding no standing at *motion for summary judgment* stage where tapes containing PII were merely "lost" while being transported on trucks and where no plaintiff had experienced identity fraud); *Blahous v. Sarrell Reg'l Dental Ctr. for Pub. Health, Inc.*, No. 2:19-CV-798-RAH-SMD, 2020 WL 4016246, at *2-3 (M.D. Ala. July 16, 2020) (breach notices only provided that the breach "'may' have" resulted in the exposure plaintiffs' PII, there was "no evidence of copied, downloaded, or removed files," and no plaintiffs experienced identity fraud following the breach); *George D., v. NCS Pearson, Inc.*, No. CV 19-2814 (JRT/KMM), 2020 WL 3642325, at *1 (D. Minn. July 6, 2020) (allegations were that hacker merely "may have had access" to "names, birthdates, and email addresses"—far less usable information than here—and no allegations of fraudulent activity experienced by any plaintiff); *Duqum v. Scottrade, Inc.*, No. 4:15-CV-1537-SPM, 2016 WL 3683001, at *4 (E.D. Mo. July 12, 2016) (emphasizing that "Plaintiffs do not allege any of the PII stolen in the breach has been used to commit any identity theft, fraud, or any other act that has resulted in harm to any plaintiff"); *Alonso v. Blue Sky Resorts, LLC*, 179 F. Supp. 3d 857, 862 (S.D. Ind. 2016) ("Importantly, not all resort customers['] [credit card numbers]…were actually exposed to the hackers' malware," there were no factual allegations that plaintiffs were among those whose credit card data was exposed, and there were no allegations of fraudulent activity experienced by plaintiffs); *Storm v. Paytime*,

While Altice suggests that the Data Breach was likely designed to commit a wire fraud (MTD at 8), this hypothetical is belied by Altice's own description of the Data Breach. According to the article relied on by Altice (*id.* at n.2), phishing campaigns that are designed to commit wire fraud "target employees with access to company finances and trick them into making wire transfers to bank accounts thought to belong to trusted partners."[3] But according to Altice's explanation of the Breach—which makes *no* mention of an attempted wire fraud—the hacker "used the stolen credentials to remotely access and, in some instances, download the employees' mailbox content." ¶ 96. If the sole objective was to trick an employee into wiring funds over email, why did the hackers *download* the contents of email boxes? Instead, because "employer's personnel records are a treasure trove of PII," it is reasonable to conclude that the hackers seized upon Plaintiffs' PII to exploit it.[4] In truth, Altice knows that the PII was a likely target of the Breach, as is evidenced by its recommendation that class members "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity." Exhibits 1-3 to Complaint at p. 3. The single password on the report containing the unencrypted PII does not make Plaintiffs' injury any less real since the hackers appear to have also obtained the password or otherwise circumvented it. ¶¶ 161-64; *see* ¶¶ 17, 73, 84. Indeed, the fact that

Inc., 90 F. Supp. 3d 359, 367 (M.D. Pa. 2015) (emphasizing that "no misuse [i.e., identity theft] was alleged"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 19-20 (D.D.C. 2014) (finding risk of identity theft speculative following a "seemingly run-of-the-mill theft" of tapes containing PII during a car break in—not a cyberattack—where thief took GPS system, stereo, and several tapes and where accessing any PII from tapes was "low" because it "require[d] specific hardware and software").

[3] https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise.

[4] *See* John Hyman, "Do Employers Have a Duty to Protect Employees' Personal Information?" (Jun. 27, 2019) https://www.workforce.com/news/do-employers-have-a-duty-to-protect-employees-personal-information.

Plaintiffs McFarlane, Mehfooz, and Paniccia experienced *actual* identity fraud following the Breach substantially supports that the PII was targeted and has been accessed. ¶¶ 17, 73, 84.

As the Sixth Circuit in *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016) explained it:

> There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals…. Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints.

Id. at 388-89. This holding is consistent with that of many courts, which have found an increased risk of future identity theft based on allegations similar to those made in the Complaint. *See, e.g.*, *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017); *Rudolph v. Hudson's Bay Co.*, No. 18-CV-8472 (PKC), 2019 WL 2023713, at *5 (S.D.N.Y. May 7, 2019) ("Consistent with *SuperValu* and *Whalen*, other courts have concluded that a data breach that includes social security numbers, names, birth dates, e-mail addresses and other contact information, employment information, online passwords and account numbers can plausibly allege a substantial risk of future harm.") (citing cases).

All Plaintiffs have alleged a substantial risk of harm as result of Altice's Data Breach.

C. Plaintiffs Have Injury-In-Fact Based on Alleged Actual Losses

All of the Plaintiffs have alleged that, as a direct result of Altice allowing their sensitive PII to be exposed to cyberhackers, Plaintiffs have been forced to expend time responding to the Breach in an attempt to mitigate its harms. ¶¶ 13-88. Specifically, Plaintiffs have had to devote notable time and cost to monitoring their financial accounts, placing credit freezes, periodically checking their credit reports, obtaining credit monitoring, registering with and reviewing resources on identitytheft.gov, changing relevant passwords, contacting financial institutions to increase the

security on accounts, scrutinizing emails for suspicious activity, and otherwise taking measures to protect themselves and mitigate the harm caused by the Data Breach. ¶¶ 18, 26, 34, 43, 50, 59, 66, 75, 85. Plaintiffs McFarlane, Mehfooz, and Paniccia have also had to spend time remedying credit card fraud as a result of unauthorized credit cards being opened in their names. ¶¶ 18, 75, 85. Mehfooz, in particular, has had to devote multiple days attempting to restore his identity and credit after a credit card that was fraudulently opened in his name damaged his credit score and interrupted his home refinancing process. ¶¶ 73-75.

In *Sackin*, this Court addressed plaintiffs' alleged injury of "lost time and money expended to mitigate threat of identity theft." *Id.* at 745. There, the Court held that plaintiffs established injury-in-fact "both regarding the risk of identity theft and remedial measures." 278 F. Supp. 3d at 747. The Court came to the same conclusion in *Rudolph v. Hudson's Bay Co.*, 2019 WL 2023713 (S.D.N.Y. May 7, 2019) where the plaintiff "identified a concrete and particularized loss based on actual time spent responding to the breach and obtaining a new debit card." *Id.* at *7 (distinguishing *Whalen* where the plaintiff "pleaded 'no specifics' about the time and effort she expended"). Indeed, courts across the country have found that the loss of time spent responding to data breaches is sufficient to establish an injury-in-fact. *See, e.g.*, *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018) ("[T]he value of one's own time needed to set things straight is a loss from an opportunity-cost perspective."); *Pedro v. Equifax, Inc.*, 868 F.3d 1275, 1280 (11th Cir. 2017) (holding that FCRA plaintiff had "alleged a concrete injury because she alleged that she 'lost time . . . attempting to resolve the credit inaccuracies'"); *Sisley v. Sprint Comm'ns Co., L.P.*, 284 Fed. Appx. 463, 466 (9th Cir. 2008) (finding "cognizable injury in fact" based on allegations of lost time).

Here, Altice specifically *recommended* that Plaintiffs take measures in response to the Data Breach. In its breach notification letter, Altice outlined steps that Plaintiffs should take "to help protect [themselves], including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert to security freeze on your credit file." *See* Exhibits 1-3 of Complaint (Altice breach notice letter to Plaintiffs) at p. 2. Altice's notice letter to Plaintiffs further stated: "It is *recommended* that you remain vigilant for incidents of fraud and identity theft by *reviewing account statements and monitoring your credit report for unauthorized activity*." *Id.* at p. 3 (emphasis added). Accordingly, Defendant's suggestion that Plaintiffs seek to "'manufacture standing by choosing to make expenditures based on hypothetical future harm,'" MTD at 11 (quoting *Clapper*, 568 U.S. at 416), is entirely baseless since Altice specifically *advised* Plaintiffs to take such steps. "Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security, *particularly when [the defendant] recommended taking these steps*." *Galaria*, 663 F. App'x at 389 (emphasis added).

D. Injury Alleged Based on Depreciation of Value of Personal Information

Plaintiffs allege the intrinsic value of their confidential information has been diminished by the Altice Data Breach. ¶ 11. Specifically, Plaintiffs allege: that their PII (including useable Social Security numbers) is a valuable commodity (¶¶ 106-114); that a market exists for Plaintiffs' confidential information, (¶ 110); that, due to the Breach, their PII was exposed to cybercriminals, (¶¶ 13-88) and; that their PII lost value as a result. These allegations are particularly relevant to Plaintiffs McFarlane, Mehfooz, and Paniccia who experienced identity theft and had credit cards fraudulently opened in their names. ¶¶ 17, 73, 84.

These allegations of injury arising from the loss of value of confidential information are sufficient to confer Article III standing. For example, in *In re Facebook Privacy Litigation*, 572 Fed. Appx. 494 (9th Cir. 2014), the court found plaintiffs plausibly alleged they experienced harm where the plaintiffs' confidential information was disclosed in a data breach, and the plaintiffs "los[t] the sales value of th[eir] [personal] information" as a result. *Id.* Similarly, in *In re Marriott International, Inc., Customer Data Sec. Breach Litig.*, No. 19-MD-2879, 2020 WL 869241 (D. Md. Feb. 21, 2020), the court correctly reasoned: "Neither should the Court ignore what common sense compels it to acknowledge – the value that personal identifying information has in our increasingly digital economy." *Id.* at *8. Further, in *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783 (N.D. Cal. May 27, 2016), the court found plaintiffs plausibly alleged injury from the loss of value of their confidential information, explaining that, for standing purposes, a plaintiff must "allege that there was either an economic market for their [personal information] *or* that it would be harder to sell their own [personal information], not both." *Id.* at *14-15; *see also Svenson v. Google, Inc.*, 2015 WL 1503429, at *5 (N.D. Cal. Apr. 1, 2015) ("Svenson's allegations of diminution in value of her [confidential information] are sufficient to show contract damages for pleading purposes."). Thus, Plaintiffs have adequately alleged injury-in-fact.

III. PLAINTIFFS STATE CLAIMS ON WHICH RELIEF CAN BE GRANTED

A complaint will survive a Rule 12(b)(6) motion when it contains "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). When ruling on such a motion, the Court must "construe the complaint liberally, accepting all factual allegations in the complaint as true, and drawing all reasonable inferences in the plaintiff's favor." *Palin v. New York Times Co.*, 940 F.3d 804, 809 (2d Cir. 2019).

Here, Altice challenges the adequacy of Plaintiffs' breach of implied contract claims and New York Labor Law claims. Defendant does not dispute the sufficiency of Plaintiffs' negligence and Cable Act claims beyond broadly challenging one theory of Plaintiffs' injury allegations. Defendant does not dispute Plaintiffs claims for declaratory and injunctive relief.

A. Plaintiffs State a Claim for Breach of Implied Contract

Under New York law, "[a] contract implied in fact may result as an inference from the facts and circumstances of the case, although not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct." *Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of New Jersey, Inc.*, 448 F.3d 573, 582 (2d Cir. 2006) (quoting *Jemzura v. Jemzura*, 36 N.Y.2d 496, 503-04 (N.Y. 1975).

While Defendant argues that an implied contract cannot be found because Plaintiffs purportedly "fail to allege any terms of the purported implied contracts," Defendant is wrong. An implied contract "rests upon the conduct of the parties and not their verbal or written words." *Parsa v. State*, 474 N.E.2d 235, 237 (1984). Here, Plaintiffs allege that: (1) they were required to provide Altice with their PII, including Social Security numbers, as part of their employment; (2) by requiring and accepting Plaintiffs' PII, Altice impliedly agreed to safeguard their PII through the use of reasonable industry standards; and (3) Altice's representations that it actively safeguards individual's information (¶¶ 131-132) further evidenced Altice's implied assurance. ¶¶ 235-37.

In *Sackin*, this Court considered nearly identical allegations and held they were sufficient:

> Plaintiffs allege conduct and a course of dealing that raise a strong inference of implied contract. TransPerfect required and obtained the PII as part of the employment relationship, evincing an implicit promise by TransPerfect to act reasonably to keep its employees' PII safe. TransPerfect's privacy policies and security practices manual—which states that the company "maintains robust procedures designed to carefully protect the PII with which it [is] entrusted"—further supports a finding of an implicit promise.

Sackin, 278 F.Supp.3d at 750. Defendant fails to address *Sackin* and fails to cite any persuasive authority to undermine its directly on-point holding.[5]

Altice next argues that Plaintiffs fail to allege "Altice's assent to be bound by any implied contracts." MTD at 17. Here again, the Court in *Sackin* addressed this very issue and held:

> While TransPerfect may not have explicitly promised to protect PII from hackers in Plaintiffs' employment contracts, "it is difficult to imagine how, in our day and age of data and identity theft, the *mandatory* receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently."

Id. (emphasis added) (quoting *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016)). Defendant ignores this relevant case law and instead relies upon the factually distinct case of *Hammond v. The Bank of New York Mellon Corp.*, No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307 (S.D.N.Y. June 25, 2010). In *Hammond*, the Court found that no implied contract existed where "none of the named Plaintiffs had any direct dealings with Defendant; Plaintiffs dealt only with Defendant's institutional clients." *Id.* at *11. This scenario is nothing like the present case, where all Plaintiffs were *employees* of Altice. As their employer, Altice assented to a contract with Plaintiffs, including the implicit agreement that Altice would use reasonable

[5] The cases cited by Defendant are inapposite. *See, e.g., Caniglia v. Chicago Tribune-New York News Syndicate, Inc.*, 612 N.Y.S.2d 146, 147 (1994) (finding breach of contract claim "too indefinite" where complaint did not allege essential elements, including whether the contract was written or oral, the provisions that defendant purportedly breached, and the rate of compensation); *Lapine v. Seinfeld*, 918 N.Y.S.2d 313, 318 (Sup. Ct. 2011) (finding no implied contract for compensation based on "bare allegations" that plaintiff submitted a book proposal to HarperCollins in response to a solicitation, but where HarperCollins rejected the proposal); *Frezza v. Google Inc.*, No. 12-CV-00237-RMW, 2012 WL 5877587, at *4-5 (N.D. Cal. Nov. 20, 2012) (accepting the *existence* of the implied contract but holding that plaintiffs failed to allege Google's *breach*); *Longenecker-Wells v. Benecard Servs. Inc*, 658 F. App'x 659, 663 (3d Cir. 2016) (conditioning its holding on the fact that plaintiffs, *unlike here*, failed to alleged company "privacy policies, codes of conduct, company security practices," etc., that supported an implicit promise to safeguard PII); *In re SuperValu, Inc.*, 925 F.3d 955, 965-66 (8th Cir. 2019) (finding no implied contract where relationship was retailer/purchaser, *not* employer/employee, and where plaintiff *was not required* to provide payment card information but instead could have paid in cash).

industry standards to protect the PII it *mandated* from Plaintiffs as part of their employment. *See McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 821 (E.D. Ky. 2019) ("Plaintiffs allege that they entered into employment agreements with Allconnect, that as a condition of their employment they had to provide personal information to Allconnect, and that Allconnect implicitly agreed to safeguard that information. This is sufficient at the pleading stage for the implied contract claim to survive."); *Castillo*, 2016 WL 9280242, at *9 ("Plaintiffs' claim is a far more realistic reflection of the mutual agreement that occurs in most data-sharing transactions: When a person hands over sensitive information, in addition to receiving a job, good, or service, they presumably expect to receive an implicit assurance that the information will be protected."). Indeed, numerous courts have found implied contracts in data breaches cases where the facts were weaker than here.[6]

Finally, Altice argues that Plaintiffs fail to allege consideration, claiming that "Plaintiffs rely solely on Altice's promise to perform pre-existing legal obligations." MTD at 18 (citing ¶ 236). But Defendant misstates Plaintiffs' implied contract allegations, which rely not only on Altice's legal obligations but also its "representations" (including those touting its data security and its commitment to secure PII, ¶¶ 131-32), as well as Altice's offer and acceptance of Plaintiffs' PII. ¶ 237. Moreover, this Court has rejected the very argument Altice posits, holding instead:

> At the motion to dismiss stage, drawing every reasonable inference in favor of Rudolph, the Court concludes that the Complaint plausibly alleges the existence of

[6] *See, e.g., Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011) ("When a customer uses a credit card in a commercial transaction, she intends to provide that data to the merchant only. Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract."); *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012) (finding breach of implied contract alleged by customers against health care services provider); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011) ("[T]he allegations demonstrate the existence of an implicit contractual relationship between Plaintiffs and Michaels, which obligated Michaels to take reasonable measures to protect Plaintiffs' financial information and notify Plaintiffs of a security breach within a reasonable amount of time."); *Rudolph*, 2019 WL 2023713, at *10 (similar).

> an implied contract, including the element of consideration. At the pleading stage, the Court is unable to discern the extent to which California's data-protection statute overlaps with any implied promise to maintain data customers' protection. This action is thus unlike *U.S. Ecology*, where the language of an express agreement was "identical" to a regulation. 92 Cal. App. 4th at 129.

Rudolph, 2019 WL 2023713, at *11. As in *Rudolph*, there is no express agreement with language identical to a regulation. And crucially, Altice disputes that its data security failures violated New York law, including New York Labor Law § 203-d. MTD at 13-15. It is untenable for Altice to argue that it was under *no* legal obligation to do more than it did while simultaneously arguing that Plaintiffs cannot bring a claim for breach of implied contract because Altice was already obligated.

Plaintiffs sufficiently alleged the existence of an implied contract. Importantly, Altice does not challenge, and thus concedes, that Plaintiffs sufficiently allege Altice's *breach* of the implied contract by failing to safeguard Plaintiffs' PII and failing to provide timely and accurate notice of the Data Breach. ¶ 238.

B. Plaintiffs State Claims Under N.Y. Labor Law § 203-d

New York Labor Law § 203-d prohibits an employer from "communicat[ing] an employee's personal identifying information to the general public." *Id.* § 203-d(1)(d). The statue defines "personal identifying information" as including, *inter alia*, Social Security number, address, and drivers' license number. *Id.*

According to the Complaint, because of Altice's inadequate cyber security practices and technologies, numerous Altice employees were confronted by, and fell victim to, a phishing campaign. As a result, certain Altice employees provided unauthorized third parties with the login credentials for Altice's corporate email accounts that contained a report with more than 52,846 current and former employees' *unencrypted* PII (including social security numbers, dates of birth,

and drivers' license numbers). ¶¶ 6-7, 95. Thus, Altice *communicated* to unauthorized parties (via email) the login credentials for an account containing Plaintiffs' unencrypted PII.

In *Sackin*, this Court considered very similar allegations—a phishing campaign whereby employee PII was disclosed to cybercriminals. The Court found that these allegations stated both a claim for negligence per se and a claim for violation of N.Y. Labor Law § 203d(1), holding:

> The Complaint sufficiently alleges breach of a statutory duty. First, New York Labor Law makes it illegal for an employer to "communicate an employee's personal identifying information to the general public." N.Y. LAB. LAW § 203-d(1)(d) (McKinney 2009). The statute defines "personal identifying information" to include: the employee's "social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, or drivers' license number." *Id.* § 203–d(1)(c). Second, Plaintiffs are within the class of persons—employees—the law is designed to protect. Third, exposure of PII is precisely the harm that the statute seeks to prevent. Even the alleged method of Defendant's breach is contemplated by the statute, which states, "It shall be presumptive evidence that a violation ... was knowing if the employer has not put in place policies or procedures to safeguard against" the disclosure of PII. *Id.* § 203–d(3).

278 F. Supp. 3d at 748-49. The Court further emphasized that § 203-d's legislative purpose was to provide "'important confidentiality safeguards for employees.'" *Id.* at 752 (quoting N.Y. Bill Jacket, 2008 S.B. 8376, Ch. 279).

The same reasoning that applied to *Sackin* applies here. As in *Sackin*, at least one Altice employee sent the login credentials for an account containing Plaintiffs' unencrypted PII to hackers. *See Sackin*, 278 F. Supp. 3d at 744 ("[A]t least one TransPerfect employee sent the information to the hackers."). Altice admits these facts. MTD at 14. While Defendant argues that the PII was not communicated to hackers, this argument is unpersuasive. Altice communicated the PII by communicating access to the digital files containing the PII. Thus, the PII *was communicated* to the unauthorized parties in the same way that information is frequently communicated electronically, by providing access to a digital file (such as Dropbox or OneDrive).

Cf. TLS Mgmt. v. Rodriguez-Toledo, 260 F. Supp. 3d 154, 160 (D.P.R. 2016) (holding that Dropbox is an electronic communication service under the Electronic Communications Privacy Act because "electronic communications are sent via Dropbox").

New York Labor Law § 203-d also prohibits an employer from "plac[ing] a social security number in files with unrestricted access." *Id.* at § 203-d(1)(c). Here, Plaintiffs sufficiently allege that Altice failed to keep its employees' Social Security numbers in files with restricted access. Altice allowed a report containing the unencrypted Social Security numbers of 52,846 employees (including numerous former employees whose data should have been purged) to be sent on its company email account and then *stored* it on the same unencrypted email inboxes. Altice then provided unauthorized third parties with access to its mailboxes and the PII report. The report containing the unencrypted employee PII was not adequately password protected, as it appears that the hackers promptly circumvented the password. ¶¶ 161-64; *see also* ¶¶ 17, 73, 84. In particular, because hackers accessed and even *downloaded* the entire account containing the unencrypted PII report, it is likely that they also obtained the password (¶ 96); even were that not so, a single document-password can be easily bypassed by numerous techniques or readily-available tools, and it would certainly pose no obstacle for cyberhackers. ¶¶ 161-64. Indeed, Altice does not dispute allegations that its security protections were negligent and, therefore, does not suggest that this password was reasonably adequate. Thus, Plaintiffs plausibly allege that Altice violated § 203-d(1)(c) by failing to keep its employees' Social Security numbers in files that restricted access.

Plaintiffs sufficiently allege that Altice violated N.Y. Lab. Law § 203-d(1)(d) and (c). It is not necessary for the Court to find that Altice violated both subsections. In the event the Court finds that Altice violated only one of the subsections, Plaintiffs can proceed on that claim alone.

C. Plaintiffs Allege Cognizable Injury

Defendant does not dispute that injury has been sufficiently alleged for Plaintiffs McFarlane, Mehfooz, and Paniccia, each of whom experienced identity theft. Instead, Altice focuses *exclusively* on Plaintiffs Cottrell, Hellyer, Mason-Draffen, Raja, Gill, and Frontera's allegations relating to lost time incurred in an attempt to mitigate the damage caused by the Data Breach. Altice argues that such injury allegations are too speculative.

As discussed *supra* at Section II.3, Plaintiffs have expended notable time monitoring their financial accounts, placing credit freezes, periodically checking their credit reports, obtaining credit monitoring, registering with and reviewing resources on identitytheft.gov, changing relevant passwords, contacting financial institutions to increase the security on accounts, scrutinizing emails for suspicious activity, and otherwise taking measures to protect themselves and mitigate the harm caused by the Data Breach. ¶¶ 18, 26, 34, 43, 50, 59, 66, 75, 85. These allegations of injury are specific, concrete, and non-speculative.

In *Sackin*, this Court addressed plaintiffs' such alleged injuries. The Court reasoned that pursuant to New York's "doctrine of avoidable consequences":

> Plaintiffs were required to take reasonable steps to mitigate the consequences of the data breach; they could not passively wait for their identities and money to be stolen. The Complaint sufficiently alleges that Plaintiffs have taken such reasonable steps, and that *they are entitled to reimbursement*.

Id. at 749 (emphasis added). The Court in *Rudolph* similarly found that plaintiff's allegations of lost time and expenses incurred in attempts to mitigate harms of data breach were "sufficient to allege injury." 2019 WL 2023713, at *9; *see also In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 2020 WL 2214152, at *4 ("Increased time spent monitoring one's credit and other tasks associated with responding to a data breach have been found by others courts to be specific, concrete, and non-speculative."); *cf. In re Gen. Motors LLC Ignition Switch Litig.*, 339 F.

Supp. 3d 262, 328 (S.D.N.Y. 2018) (holding that loss of personal time constituted damages for violation of statute that, as with Plaintiffs' Cable Act claim, included statutory damages).

Here, Altice specifically notified Plaintiffs that their PII was compromised in the Breach and *recommended* that Plaintiffs take mitigating measures, including "reviewing account statements and monitoring your credit report for unauthorized activity." Complaint's Exhibit 3 at p. 3. Accordingly, this is *nothing* like the situation in *Willey v. J.P. Morgan Chase, N.A.*, No. 09 CIV. 1397(CM), 2009 WL 1938987 (S.D.N.Y. July 7, 2009), a case cited by Defendant, where the Court reasoned that "the fact that Willey himself was not notified that his data had been lost—which admits of the inference that he was not one of the 2.6 million customers affected by Chase's improper disposal of data—fairly implies that he could not have been damaged at all." *Id.* at *10. Here, however, "[w]here Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse…before taking steps to ensure their own personal and financial security, *particularly when [the defendant] recommended taking these steps*." *Galaria*, 663 F. App'x at 389 (emphasis added).

In addition, *all* Plaintiffs sufficiently allege redressable injury due to the diminution of their confidential information (¶¶ 11, 106-114). *See e.g.*, *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1224 (N.D. Cal. 2014) (finding it plausible "that a company's security practices have economic value" and finding that plaintiffs had "plausibly pleaded" benefit of the bargain losses where defendant allegedly failed to provide adequate security); *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) (finding allegations that plaintiffs' personal information is a "valuable commodity" and theft of this information reduces

its value sufficient to plead damages for a breach of contract claim).[7] Further, *all* Plaintiffs allege statutory damages, including liquidated damages. ¶¶ 222, 231-32. Because Defendant does not dispute that either of these injury theories are sufficiently alleged, dismissal for lack of injury is unwarranted. *Cf. Fero v. Excellus Health Plain, Inc.*, 236 F. Supp. 3d 735, 785-86 (W.D.N.Y. 2017), *on reconsideration sub nom.*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018) (rejecting Defendants' "wholesale" challenge of Plaintiffs' damages theories rather than challenging damages "under each claim," holding: "Defendants make no attempt to identify whether Plaintiffs have sufficiently pleaded damages for purposes of each of their claims. Given that it is the movant's burden to show why dismissal is warranted on a 12(b)(6) motion, the Court denies the Excellus Defendants' motion, to the extent it is predicated on an alleged failure to plead any cognizable damages.").

Plaintiffs has plausibly alleged numerous theories of non-speculative injury.

IV. PLAINTIFFS ARE NOT COMPELLED TO ARBITRATE THIS ACTION

While Defendant cites authorities emphasizing a strong policy favoring arbitration, the Supreme Court has repeatedly made clear that the Federal Arbitration Act ("FAA") was designed "to make arbitration agreements as enforceable as other contracts, *but not more so*." *Volt Info. Scis., Inc. v. Bd. of Trustees of Leland Stanford Junior Univ.*, 489 U.S. 468, 478 (1989) (emphasis added) (citation omitted). "Accordingly, we have recognized that the FAA does not require parties to arbitrate when they have not agreed to do so." *Id.*

[7] Plaintiffs also allege that Altice's post-breach security measures are still inadequate and request appropriate declaratory and injunctive relief to protect Plaintiffs from future injury. ¶¶240-46. *See, e.g., In re Adobe Sys.*, 66 F. Supp. 3d at 1222-23 ("Plaintiffs seek a declaration clarifying Adobe's *ongoing* contractual obligation to provide reasonable security. Plaintiffs' claim thus requests precisely the type of relief that the Declaratory Judgment Act is supposed to provide: a declaration that will prevent future harm from ongoing and future violations before the harm occurs."); *In re Yahoo! Inc. Customer Data Security Breach Litig.*, 313 F. Supp. 3d 1113, 1139 (N.D. Cal. 2018) (allowing declaratory relief to proceed in data breach case).

"Courts deciding motions to compel . . . draw[] all reasonable inferences in favor of the non-moving party." *Meyer v. Uber Techs., Inc.*, 868 F.3d 66, 74 (2d Cir. 2017) (citation omitted).

A. This Action Falls Outside the Scope of the Arbitration Clause

When deciding whether to compel arbitration, courts must consider "(1) whether the parties have entered into a valid agreement to arbitrate, and if so, (2) whether the dispute at issue comes within the scope of the arbitration agreement." *Id.* at 128. If both conditions are met, the Court must send the case to arbitration. *Plazza v. Airbnb, Inc.*, 289 F. Supp. 3d 537, 547 (S.D.N.Y. 2018). If either is missing, the nonmoving party cannot be forced to arbitrate the dispute. *In re Am. Express Fin. Advisors Sec. Litig.*, 672 F.3d 113, 127 (2d Cir. 2011) ("[A] party cannot be required to submit to arbitration any dispute which he has not agreed so to submit.") (quoting *Howsam v. Dean Witter Reynolds, Inc.*, 537 U.S. 79, 83 (2002)).

Here, because Plaintiffs' claims arise from their employment at Altice and *not* their cable service, Plaintiffs' claims fall outside the scope of the arbitration clause contained within Optimum's General Terms and Conditions of Service ("Terms of Service").

Plaintiffs do not contest that the arbitration provision in the Terms of Service is broad, by generally providing for the arbitration of "any and all disputes arising between [the customer] and Cablevision." Heberer Declaration in Support of Motion to Compel (Dkt. No. 49) ("Heberer Decl.") at Exh. 1-6. However, the Second Circuit has held that even in the face of a broad arbitration provision, "claims that present *no question involving construction of the contract*, and no questions in respect of the parties' rights and obligations *under it*, are beyond the scope of the arbitration agreement." *Collins & Aikman Prods. Co. v. Bldg. Sys., Inc.*, 56 F.3d 16, 23 (2d Cir. 1995) (emphasis added). Thus, when faced with a broad arbitration provision, the Court must: (1) determine if "the dispute is in respect of a matter that, on its face, is clearly collateral to the contract," and (2) if so, ask "whether the claim alleged implicates issues of contract construction

or the parties' rights and obligations under it[.]" *Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17, 36 (2d Cir. 2002) (quoting *Collins*, 56 F.3d at 23).

In *Specht*, the Second Circuit applied this analysis. First, the Court held:

> To begin with, we find that the underlying dispute in this case—whether defendants violated plaintiffs' rights under the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act—involves matters that are clearly collateral to the Communicator license agreement…. [O]n its face, the Communicator license agreement governed disputes concerning Netscape's browser programs only, *not* disputes concerning a plug-in program like SmartDownload.

306 F.3d at 36. In so finding, the Court emphasized that the license agreement contained a merger clause and reasoned that "defendants' express desire to limit the reach of the respective license agreements, combined with the absence of reference to SmartDownload in the Communicator license agreement, suggests that a dispute regarding defendants' allegedly unlawful use of SmartDownload is clearly collateral to the Communicator license agreement." *Id.* Second, the Court held that plaintiffs' claims "present no question involving construction of the [Communicator license agreement], and no questions in respect of the parties' rights and obligations under it." *Id.* at 38 (quoting *Collins*, 56 F.3d at 23). For this determination, the Court found that "Plaintiffs' allegations consistently distinguish and isolate the functions of SmartDownload in such a way as to make it clear that it is through SmartDownload, not Communicator, that defendants committed the abuses that are the subject of the complaints." *Id.*

Here, first, as in *Specht*, Plaintiffs' dispute is collateral to the Terms of Service. Nowhere is a data breach pertaining to *employees'* PII discussed in the Terms of Service, which instead discuss terms relating to Optimum's cable service. Indeed, the Terms of Service state: "THIS Agreement contains a binding arbitration provision … that affects your rights under this agreement ***with respect to all services***." Heberer Decl. at Exhs. 1, 13; *see also id.* at Exh. 6 ("*Subscriber*…agree[s] to be bound to these [Terms of Service] ***with respect to all Optimum***

services….").[8] After all, the terms are entitled "Terms and Conditions ***of Service***." *Id.* at Exhs. 1-6 (emphasis added). Even the arbitration clause states: "Because ***the Service(s)*** provided to You involves interstate commerce, the Federal Arbitration Act ("FAA"), not state arbitration law, shall govern…." *Id.* (emphasis added) Such language demonstrates that the agreement, and its arbitration clause, were intended to cover claims arising from use of the cable service *not* arising from employment. As in *Specht*, the absence of language addressing the matter in dispute is dispositive given that the Terms of Service contains a merger clause attesting the completeness of the agreement. *Id.*; *see Specht*, 306 F.3d at 36; *see also FUJIFILM N. Am. Corp. v. Geleshmall Enterprises LLC*, 239 F. Supp. 3d 640, 649-50 (E.D.N.Y. 2017) (finding dispute collateral to contract where "parties did not agree to arbitrate gray market claims"); *Armor All/STP Prod. Co. v. TSI Prod., Inc.*, 337 F. Supp. 3d 156, 169-70 (D. Conn. 2018) ("The allegations in the amended complaint are "clearly collateral" to the Consulting Agreement…. The Consulting Agreement does not concern Plaintiff's rights to particular trademarks, trade dress, or creative works, the primary subject of this dispute.").

Second, as in *Specht*, the claims "present no question involving construction of the [Terms of Service], and no questions in respect of the parties' rights and obligations under it," and Plaintiffs' allegations "make it clear that it is through" Plaintiffs' employment *not* their use of

[8] The other documents submitted by Altice further indicate that the scope of the arbitration is limited to issues relating to service. *See, e.g.*, Heberer Decl. at Exhs. 10, 11, 14, 15 ("***Your use of the Service*** is Subject to Binding Arbitration…."); *id.* at Exh. 12 ("THE TERMS OF SERVICE ***GOVERNING YOUR USE OF ALL OPTIMUM SERVICES*** HAVE RECENTLY BEEN REVISED TO INCLUDE THE FOLLOING BINDING ARBITRATION PROVISION…"); *id.* at Exh. 7 ("THESE CABLEVISION TERMS OF SERVICE ***GOVERNING YOUR USE OF iO TV*** INCLUDE A BINDING ARBITRATION PROVISION…); *id.* at Exh. 8 ("THESE CABLEVISION TERMS OF SERVICE ***GOVERNING YOUR USE OF OPTIMUM VOICE*** INCLUDE A BINDING ARBITRATION PROVISION….); *id.* at Exh. 9 ("THESE CABLEVISION TERMS OF SERVICE ***GOVERNING YOUR USE OF OPTIMUM ONLINE***…INCLUDE A BINDING ARBITRATION PROVISION….) (emphasis added in all).

Optimum cable services, "that defendant[] committed the abuses that are the subject of the complaints." *Specht*, 306 F.3d at 38. Indeed, the Complaint explains that the exposure of Plaintiffs' PII arises from, and is a result of, Plaintiffs' employment at Altice and Altice's affiliate companies. To be sure, the letters Altice sent to *every* Plaintiff, each of whom is a former employee of Altice or an Altice affiliate, provided:

> Unfortunately, we are contacting you about an email phishing incident that may have involved some of your personal information ***as a former employee of Altice USA***, its subsidiaries or predecessor companies….
>
> ***
>
> **What information was involved?**
> During our investigation, we learned in January 2020 that one of the downloaded mailboxes contained a password protected report that contained personal information, including name, ***employment information***, Social Security number, date of birth and, in some instances, driver's license number. ***As a former employee***, ***your personal information was included in this report***.

Exhibits 1-3 of Complaint (emphasis added). Thus, by *Altice's own representation*, for every Plaintiff, their personal information was exposed because they were each "former employee[s]" of Altice or its affiliates. In fact, the notice letters Altice provided to state attorneys general only included two options: "As a *current employee*, your personal information was included in this report" or "As a *former employee*, your personal information was included in this report." ¶ 97 (emphasis added). There was absolutely *no* option for "customer" or "former customer" in Altice's letter. Further, Altice has admitted that the report accessed and downloaded by hackers contained the PII of *all* current employees and many former employees. ¶¶ 98-99. Indeed, it is evident that the stolen report was *employment* related and contained "*employment* information." ¶ 96; Exhs. 1-3 of Complaint. This is confirmed by Altice's representation in its Motion to Dismiss that the "report contained data on employees and some former employees." MTD at 8. While some employees also subscribed to Altice services, this does not change the fact that, as Altice admits,

Plaintiffs' PII was exposed because they were "former employee[s]" of Altice. ¶ 97. Because Plaintiffs' claims arise from their employment at Altice and "present no question involving construction of the [Terms of Service], and no questions in respect of the parties' rights and obligations under it," the claims fall outside the scope of the arbitration clause. *Specht,* 306 F.3d at 38.

Indeed, "courts determining whether 'clearly collateral' claims are arbitrable – even when the arbitration clause is broad – focus on whether adjudicating the claims would require construction of the contract." *Armor All/STP Prod. Co.*, 337 F. Supp. 3d at 170 (D. Conn. 2018) (quoting *WorldCrisa Corp. v. Armstrong*, 129 F.3d 71, 74 (2d Cir. 1997)); *see, e.g., Benihana of Tokyo, LLC v. Benihana Inc.*, 73 F.Supp.3d 238, 253-57 (S.D.N.Y. 2014); *Kuklachev v. Gelfman*, 600 F.Supp.2d 437, 461-67 (E.D.N.Y. 2009). Thus, as the Eastern District of New York has held:

> Although the burden is on FUJI to show that the claims are not subject to arbitration despite the broad arbitration clause, FUJI has met that burden because the gray market *claims exist separate and apart* from the conduct that is the subject of the 2014 Agreement…. *The important point is that FUJI's gray market claims exist outside of the 2014 Agreement. If that Agreement never existed, FUJI would have the same claims it has now under the Lanham Act.*

FUJIFILM N. Am. Corp., 239 F. Supp. 3d at 649-50 (emphasis added).

Here, Plaintiffs' claims relating to Altice's inadequate protections over PII and wrongful exposure of PII to unauthorized parties exist entirely outside of and apart from the Terms of Service, and Plaintiffs "would have the same claims" if the Terms of Service "never existed." *Id.* Even Plaintiffs' Cable Act claim is outside the scope of the arbitration clause because this claim does not require "construction of" the Terms of Service nor does it involve "questions in respect of the parties' rights and obligations under it." *Specht,* 306 F.3d at 36 ("[C]laims that present no question involving construction of the contract, and no questions in respect of the parties' rights and obligations under it, are beyond the scope of the arbitration agreement.") Indeed, under the

Cable Act, Altice owes specific obligations to secure the personal information (including Social Security numbers) of "*any* subscriber"; this includes any subscriber who is also an employee. Even Altice acknowledges and represents in its Customer Privacy Notice[9] that claims like the present claims, including Cable Act claims, *fall outside the scope of the arbitration clause. See* ¶ 131 (discussing Altice's obligations under the Cable Act and stating that if Altice fails "to prevent unauthorized access to [personally identifiable] information…you may be entitled to bring a civil action ***in a federal court***, which may award actual, liquidated, and punitive damages, fees and costs, and other remedies that may be available."). Moreover, based on the breach notification letters Altice sent to *every* Plaintiff, it is undisputed that the exposure of Plaintiffs' PII arises from Plaintiffs' *employment* at Altice. ¶¶ 96-97. Simply put, this action does *not* arise from Plaintiffs' use of Optimum cable services and does *not* raise a question in respect to the parties' rights and obligations under the Terms of Service.

The cases cited by Defendant are inapposite and do not support Altice's position here. In *Paramedics Electromedicina Comercial, Ltda v. GE Med. Sys. Info. Techs., Inc*., 369 F.3d 645 (2d Cir. 2004) the Court made the unsurprising conclusion that claims were arbitrable where the agreement "govern[ed] the relationship between the companies regarding the distribution, sale, and service of GEMS–IT's products in Brazil" and the allegations were that defendant "circumvented [plaintiff] as the distribution agent for certain products that were imported into Brazil." *Id.* at 654. In the out-of-circuit case *Drews Distrib., Inc. v. Silicon Gaming, Inc.*, 245 F.3d 347 (4th Cir. 2001), the court found that "a dispute over payment for 200 video gambling machines" fell within the distribution agreement's arbitration provision where even plaintiffs

[9] The Customer Privacy Notice is incorporated in the Terms of Service. *See* Heberer Decl. at Exhs. 1-6.

conceded that the agreement "control[ed] the rights of the parties as to the sale of these Odyssey machines." *Id.* at 350-51. Similarly, in *Anders v. Hometown Mortg. Servs., Inc.*, 346 F.3d 1024 (11th Cir. 2003), the court found claims for violations of the Real Estate Settlement Procedures Act and Truth in Lending Act arbitrable where the plaintiff had signed an arbitration agreement as part of the closing documents between plaintiff and defendants. The other cases relied upon by Altice are also distinguishable and unpersuasive. *See, e.g.*, *Belke v. Merrill Lynch, Pierce, Fenner & Smith*, 693 F.2d 1023, 1028 (11th Cir. 1982), *abrogated by Dean Witter Reynolds, Inc. v. Byrd*, 470 U.S. 213 (1985) (compelling arbitration of plaintiffs' claims for mismanagement of stock portfolio where Customer Agreement with broker included provision that "any controversy between us arising out of your business" would be arbitrated); *Coenen v. R. W. Pressprich & Co.*, 453 F.2d 1209, 1210-12 (2d Cir. 1972) (compelling arbitration for claims against broker relating to the transfer of stock where plaintiff applied for membership in the New York Stock Exchange and thereby agreed to arbitrate "'[a]ny controversy between… members…arising out of the business of such member…,'" "with full knowledge that he had a claim against Pressprich and that Pressprich was a Stock Exchange member."); *Cara's Notions, Inc. v. Hallmark Cards, Inc.*, 140 F.3d 566, 569-71 (4th Cir. 1998) (considering "arm's length" contracts between businesses and finding that the arbitration clause within a second contract applied to disputes involving all stores).

None of the cases relied on by Defendant address what we have here, which is an entirely *separate* relationship between the parties that is not addressed in the agreement containing an arbitration clause. As discussed *supra* at 25-27, it was the separate employment relationship that caused Plaintiffs' PII to be exposed in the Data Breach, as Altice admits. *See* ¶ 97 ("As a former employee, your personal information was included in this [compromised] report."). Thus, the issue before the Court is: whether an arbitration clause within a boilerplate Terms of Service, relating to

certain Plaintiffs' use of cable services, applies to claims relating to Plaintiffs' entirely separate employer/employee relationship with Altice. Second Circuit authority dictates that it does not so apply. *See supra* at 23-28. Under Defendant's theory, Altice could use the arbitration provision within its Terms of Service agreement to compel arbitration over its employees' potential workers compensation claims, ERISA claims, etc., if those employees used Optimum cable services. *Cf. Smith v. Steinkamp*, 318 F.3d 775, 777 (7th Cir. 2003) (J. Posner) (discussing the "absurd results" that would ensue if an arbitration clause truly applied to any dispute even those "standing free from" the agreement). Altice fails to present cases to support the overbroad interpretation they advocate.

Even Altice seems to understand the stretch it is advocating. Originally, in response to the potential consolidation of two related actions, Altice came forward with an *employment* related arbitration agreement signed by then-plaintiff Brittany Wiley. *See* Wiley Agreement, attached as Exh.1 to the Declaration of A. Brooke Murphy, filed herewith. Altice used that arbitration agreement to argue that Wiley's action could not be consolidated with Hellyer's action because only Wiley was subject to binding arbitration. Dkt. No. 10. In response to Altice's submission, the claims of then-plaintiff Wiley were dismissed. However, Plaintiff Hellyer's action proceeded and was consolidated based on Altice's contention that Hellyer's claims were *not* subject to arbitration. *Id.* Months later, Altice reversed course and raised the present novel argument that Plaintiff Hellyer and other Plaintiffs are required to arbitrate their claims based on their use of Optimum cable services pursuant to the Terms of Service. This chain of events, and complete reversal by Altice, exposes the tenuousness of the argument Defendant now makes.

The Terms of Service, which governs the service provider/customer relationship and the use of Optimum's cable service, does not require Plaintiffs to arbitrate unrelated claims that derive

from their wholly distinct employer/employee relationship with Altice. Accordingly, Defendant's motion to compel arbitration should be denied.

B. Plaintiffs Never Manifested Assent to Arbitrate Disputes Arising from Their Employment at Altice

A key question when considering a motion to compel is "whether the parties have indeed agreed to arbitrate." *Schnabel v. Trilegiant Corp.*, 697 F.3d 110, 118 (2d Cir. 2012). Here, even were the Court to conclude that this dispute falls within the scope of the arbitration provision, Defendant has failed to show that Plaintiffs agreed to arbitrate such claims.

"[T]o be binding, a contract requires a 'meeting of the minds' and 'a manifestation of mutual assent.'" *Starke v. SquareTrade, Inc.*, 913 F.3d 279, 288 (2d Cir. 2019) (citations omitted). "The manifestation of mutual assent must be sufficiently definite to assure that the parties are truly in agreement with respect to all material terms." *Id.* at 289. Actual notice of contractual terms is not required when the party is on inquiry notice of the terms. *Id.* "Inquiry notice is actual notice of circumstances sufficient to put a prudent man upon inquiry." *Specht*, 306 F.3d at 30 n. 14 (citation omitted). The "[c]larity and conspicuousness of [the] terms are important" to a determination of whether a prudent offeree was on inquiry notice of the terms. *Id.* at 30. Indeed, the party must be "meaningfully informed of the contractual terms at stake." *Ward v. Cross Sound Ferry*, 273 F.3d 520, 523 (2d Cir. 2001).

The case of *Wexler v. AT & T Corp.*, 211 F. Supp. 3d 500, 504 (E.D.N.Y. 2016), is particularly instructive as it applied Second Circuit law to an arbitration clause similar to the one presented here. In *Wexler*, the plaintiff's cell phone service agreement included a broad arbitration clause that applied to the defendant and its affiliates and required arbitration of "all disputes and claims between [them]." *Id.* at 501. The plaintiff sued the defendant for violations of the Telephone Consumer Protection Act due to unsolicited text message advertisements for television and internet

service that the plaintiff received from one of the defendant's subsidiaries after the expiration of her cell phone contract. *Id.* at 502. The court declined to compel arbitration of the plaintiff's claims, finding both that the arbitration clause was "unlimited in scope" and that the plaintiff's claim was wholly unrelated to her cell phone service. *Id.* at 504-05. The court held:

> But the words expressed [in the agreement] must be judged according to "what an objective, reasonable person would have understood [them] to convey." *Leonard v. Pepsico, Inc.*, 88 F.Supp.2d 116, 127 (S.D.N.Y.1999) (citing *Kay–R Elec. Corp. v. Stone & Webster Constr. Co.*, 23 F.3d 55, 57 (2d Cir.1994)). Notwithstanding the literal meaning of the clause's language, *no reasonable person would think that checking a box accepting the "terms and conditions" necessary to obtain cell phone service would obligate them to arbitrate literally every possible dispute he or she might have with the service provider*, let alone all of the affiliates under AT & T Inc.'s corporate umbrella—including those who provide services unrelated to cell phone coverage. *Rather, a reasonable person would be expressing, at most, an intent to agree to arbitrate disputes connected in some way to the service agreement with Mobility*. As explained above, Wexler's claims are not so connected. If a company wishes to bind its customers to something broader, it must take steps to secure something that a reasonable person would understand as an objective expression of his or her agreement. [*Id.*]

As in *Wexler*, "no reasonable person would think" that signing a cable installation form "accepting the 'terms and conditions'" of the cable service would obligate them to arbitrate claims wholly unrelated to the cable service but instead arising from their employment. *Id.* It would be particularly difficult to find such assent here, given that the Terms of Service indicates that the agreement's scope is limited to issues relating to *service*. *See* Exhs. 1-6 to Heberer Decl. ("***Subscriber*** agrees to be bound by the terms of service ***for the applicable Optimum service***…"); *id.* ("Because ***the Service(s)*** provided to You involves interstate commerce, the Federal Arbitration Act ("FAA"), not state arbitration law, shall govern…."). In fact, the paper workorders signed by Plaintiffs state: "YOUR ***USE OF THE SERVICES*** IS SUBJECT TO A BINDING ***ARBITRATION PROVISION THAT AFFECTS YOUR RIGHTS UNDER THIS AGREEMENT WITH RESPECT TO ALL SERVICES***." Heberer Decl. at Exh. 10 (emphasis

added). Similarly, the iPad workorders signed by Plaintiffs state: "YOUR ***USE OF THE SERVICE*** IS SUBJECT TO A BINDING ***ARBITRATION PROVISION that affects your rights under this Agreement with respect to all Services***." Heberer Decl. at Exh. 11 (emphasis added).[10] Plaintiff McFarlane never signed any document that even attempted to incorporate the broader Terms and Conditions. *See* Heberer Decl. at ¶¶ 27, 40; *id.* at Exhs. 10-11, 22. And Altice has failed to locate *any* document signed by Plaintiff Frontera. Heberer Decl. at ¶ 60.

While Defendant cites cases that purportedly enforced Altice's arbitration clause "under the same circumstances as presented in the instant case" (MTCA at 13), this is simply false. The cases referenced by Altice dealt with disputes that *actually derived from* those plaintiffs' use of cable service. *See, e.g., Krafczek v. Cablevision Sys. Corp.*, No. 2:17-cv-02915-JMA-SIL, 2018 WL 8918077, at *3-4 (E.D.N.Y. Apr. 25, 2018) (customer class action alleging deceptive billing practices by Cablevision for its services); *Serrano v. Cablevision Sys. Corp*., 863 F. Supp. 2d 157, 161 (E.D.N.Y. 2012) (customer class action bringing claims relating to quality and speed of internet service); *Hammer v. Cablevision of Boston, Inc*., 18 Misc. 3d 727, 728 (N.Y. Just. Ct. 2007) (customer raising claims related to changes in channels provided through cable service). These courts did *not* find assent to arbitrate claims based on the Altice's Terms of Service where the claims were entirely unrelated to the plaintiffs' use of cable service.

Altice further argues that Plaintiffs assented to the arbitration clause by their continued use of cable services after receiving an annual Service Terms and Information insert in their Optimum billing statements. This contention is undermined by controlling law. The Second Court has held that "[t]he conduct of a party is not effective as a manifestation of his assent unless he intends to

[10] Altice presents Exhibit 10 as a sample of the back of the paper workorders signed by Plaintiffs and Exhibit 11 as a sample of the iPad workorders signed by Plaintiffs. Heberer Decl. at ¶ 27.

engage in the conduct and knows or has reason to know that the other party may infer from his conduct that he assents." *Schnabel*, 697 F.3d at 120 (citation omitted). Thus, manifestation of assent can be found only if the party "is on inquiry notice of [the terms] and assents to them *through conduct that a reasonable person would understand to constitute assent*." *Starke*, 913 F.3d at 288 (emphasis added).

Applying this law to the present case, "a reasonable person" would not understand using a cable service "to constitute assent" to arbitrate claims wholly unrelated to that service but instead arising from his/her employment. *See Stark*, 913 F.3d at 289. Nor would Plaintiffs have known or had reason to know that Altice "may infer from" their continued use of cable services that they assent to arbitrate claims arising from and related to their employment. *See Schnabel*, 697 F.3d at 120. The fact that the Terms of Service were provided to Plaintiffs in their Optimum "*subscriber invoices*" further supports a lack of assent by Plaintiffs. *See* Heberer Decl. at ¶ 34. Plaintiffs would have no reason to think that a Service Terms and Information insert in an Optimum billing statement would contain material terms that could substantially impact their ability to redress disputes created from their employment at Altice. *See Specht*, 306 F.3d at 29 ("[A]n offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious.") (citation omitted).

Altice provides no persuasive legal support for their argument. Instead, Defendant again cites cases analyzing assent through continued use of service where the disputes were, in fact, related to that use of service. *See* MTCA at 14-15. These cases are unconvincing here because the harm was not a result of Plaintiffs' use of Altice services but was instead the result of Plaintiffs' *employment* at Altice. Here, there is no "course of dealing between the parties" nor "industry

practices" to suggest that by continuing their cable services Plaintiffs were assenting to arbitrate claims resulting from their employment. *See Schnabel*, 697 F.3d at 124. This is unlike the cases cited by Defendant where course of dealing and industry practices can be found to support the arbitrability of service-related claims. *See, e.g.*, *Olsen v. Charter Commc'ns, Inc.*, Nos. 18cv3388 (JGK), 2019 WL 3779190, at *5 (S.D.N.Y. Aug. 9, 2019) ("A billing statement, which 'contains information at the heart of the *service relationship*'… is a method that could be 'well-suited' for notifying *customers* about updates to Charter's terms and conditions") (emphasis added). Significantly, Defendant cites *no* case holding that continued *service* constitutes manifest assent to arbitrate claims arising from a person's *employment* at a company.

"'Th[e] principle of knowing consent applies with particular force to provisions for arbitration.'" *Specht*, 306 F.3d. at 30 (citation omitted). Altice has failed to demonstrate Plaintiffs' consent to arbitrate the claims raised in the Complaint.

V. CONCLUSION

For the reasons stated herein, Plaintiffs respectfully request that the Court deny Defendant's Motions in their entirety. In the event the Court dismisses the Complaint in whole or in part, Plaintiffs respectfully request leave to amend. *See* Fed. R. Civ. P. 15(a)(2) (leave to amend shall be "freely" given); *Shaw v. Empire Stock Transfer Inc.*, 381 F. Supp. 3d 286, 292-93 (S.D.N.Y. 2019) ("Where the possibility exists that [a] defect can be cured, leave to amend should normally be granted.") (permitting leave to amend upon granting motion to dismiss).

Dated: August 31, 2020

Respectfully submitted,

/s/ *A. Brooke Murphy*

A. Brooke Murphy
(admitted *pro hac vice*)
William B. Federman
(S.D. New York #WF9124)
Interim Lead Class Counsel
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
abm@federmanlaw.com
wbf@federmanlaw.com

Interim Lead Class Counsel

Richard A. Acocelli
1500 Broadway, 16th Floor
New York, New York 10036
Tel: (212) 682-3025
Fax: (212) 682-3010
racocelli@weisslawllp.com

Cornelius P. Dukelow
ABINGTON COLE + ELLERY
320 South Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
Telephone and Facsimile: (918) 588-3400
cdukelow@abingtonlaw.com

Additional Plaintiffs' Counsel

CERTIFICATE OF SERVICE

I hereby certify that on August 31, 2020, a true and correct copy of the foregoing was electronically filed with the Clerk of Court using CM/ECF. Copies of the foregoing document will be served upon interested counsel via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/ *A. Brooke Murphy*
A. Brooke Murphy